ABSTRACT OF THE DISCLOSURE

A cryptographic processing method in which dependence of cryptographic processing process and secret information on each other is cut off; and in which, when a scalar multiplied point is calculated from a scalar value and a point on an elliptic curve in an elliptic curve cryptosystem, a value of a bit of the scalar value is judged; and in which operations on the elliptic curve are executed a predetermined times and in a predetermined order without depending on the judged value of the bit.